

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Prins Clauslaan 20
TEL 070 - 381 13 00 FAX 070 - 381 13 01 E-MAIL info@cbpweb.nl INTERNET www.cbpweb.nl

ALGEMENE BEVINDINGEN

naar aanleiding van de onderzoeken door het CBP
naar de bijzondere politieregisters van
Criminele Inlichtingen Eenheden in 2003/2004

Het College bescherming persoonsgegevens (CBP) publiceert in zijn serie Rapporten resultaten van onderzoek naar de stand van zaken bij de bescherming van persoonsgegevens in organisaties en sectoren. De Rapporten zijn gebaseerd op onderzoeken uitgevoerd door of in opdracht van het CBP. Door publicatie van deze Rapporten vraagt het CBP aandacht voor feiten die de persoonlijke levenssfeer van de burger raken. Het CBP wil hiermee bewustwording en naleving van de normen voor de bescherming van persoonsgegevens bevorderen.

Algemene bevindingen naar aanleiding van de onderzoeken door het CBP naar de bijzondere politieregisters van criminele inlichtingen eenheden in 2003/2004, Rapport 2, College bescherming persoonsgegevens, Den Haag, september 2004

© Niets uit deze uitgave mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke wijze dan ook, zonder voorafgaande schriftelijke toestemming van het College bescherming persoonsgegevens.

INHOUDSOPGAVE

Samenvatting

- I Inleiding
- II Bevindingen naar aanleiding van de onderzoeken
 - 1. Inhoud van de gegevens
 - 2. Codering
 - 3. Bewaartermijnen
 - 4. Onderscheid in categorieën geregistreerden
 - 5. Definitieve vaststelling gespreksverslagen
 - 6. Toegang
 - 7. Logging database
 - 8. Verstrekkingen
 - 9. Samenhang van inhoudelijke en technische/organisatorische aspecten
- III De reacties van de korpsen
- IV Conclusie

Samenvatting

Het College bescherming persoonsgegevens (CBP) heeft in 2003/2004 onderzoek gedaan naar de bijzondere politieregisters die door de Criminele Inlichtingen Eenheden (CIE'en) bij de regionale politiekorpsen worden gehouden. Het CBP is ingevolge de Wet politieregisters (Wpolr) toezichthouder op de werking van de politieregisters en ziet in die positie, gelet op de gevoeligheid van de door de CIE verwerkte informatie, een bijzondere verplichting om met name ook toe te zien op de inhoud van de bijzondere politieregisters.

Het CBP heeft bij acht korpsen onderzoek gedaan door middel van een steekproef in de registers bij de CIE, te weten het informantenregister, het register zware criminaliteit en het voorlopig register. Vanwege de beperking van het onderzoek ter plaatse tot één dag betrof het aantal onderzochte gespreksverslagen en mutaties een gering aantal. Daarnaast zijn technische en organisatorische aspecten onderzocht die aanvullende informatie geven op het beeld van de inhoud van de registers.

Het algemene beeld dat uit het onderzoek naar voren kwam is als overwegend positief aan te duiden. De onderzochte inhoudelijke aspecten bleken over het algemeen in orde. Wat betreft de onderzochte technische en organisatorische aspecten viel op dat op een aantal punten niet wordt voldaan aan de voorschriften die door de wet- en regelgeving worden gesteld. Veel van de korpsen geven aan dat zij, in afwachting van een landelijk in te voeren informatiesysteem, op die punten geen aanpassingen uitvoeren ten aanzien van de huidige systemen en gehanteerde werkwijzen.

De algemene bevindingen op de belangrijkste onderdelen kunnen als volgt worden omschreven.

1. **inhoud van de gegevens**

Het CBP heeft met name de juistheid en volledigheid van de informatie onderzocht en vergeleken of de in het register zware criminaliteit en het voorlopig register opgenomen mutaties (nettoverslagen) overeenkwamen met de gespreksverslagen in het informantenregister (brutoverslagen) waaruit zij afkomstig waren. Over het geheel genomen was de verslaglegging consistent en voldoende duidelijk en stemden de vergelijking van netto- en brutoverslagen overeen. Ook heeft het CBP geen informatie in de registers aangetroffen die niet door de CIE behoort te worden verwerkt.

2. **codering**

Het gebruik van de verplicht voorgeschreven evaluatie- en afhandelingscodes waarmee de CIE-informatie wordt gecodeerd is getoetst. Codering bleek door alle onderzochte korpsen consequent te worden vermeld en kwam het CBP doorgaans niet onaannemelijk voor. De sedert 4 juli 2003 gewijzigde coderingstabel bleek echter slechts bij één korps te zijn ingevoerd. Twee andere korpsen gaven aan deze tabel alsnog te zullen hanteren.

3. **bewaartermijnen**

Het CBP heeft hier de maximale bewaartermijn (marginaal) getoetst die geldt voor het register zware criminaliteit (5 jaar) en voor het voorlopig register (6 maanden). In het register zware criminaliteit is vrijwel geen overschrijding aangetroffen. Bij het voorlopig register werd meerdere malen een betrekkelijk geringe overschrijding geconstateerd.

4. onderscheid in categorieën geregistreerden
De Wpolr schrijft voor dat wat betreft in het register zware criminaliteit en voorlopig register geregistreerde personen onderscheid moet worden gemaakt tussen verdachten, betrokkenen en contacten. Geen van de onderzochte korpsen maakte dit drieledig onderscheid. De meeste korpsen maken slechts onderscheid tussen subjecten (waaronder verdachten en betrokkenen begrepen worden) en contacten.
5. definitieve vaststelling gespreksverslagen
Bij de meeste korpsen bleek dat wijziging van gespreksverslagen na vaststelling daarvan niet door het systeem wordt uitgesloten. Door enkele korpsen is dit na het onderzoek alsnog aangepast.
6. toegang
Bij alle onderzochte korpsen bleek dat (veel) meer functionarissen rechtstreeks toegang hadden tot het informantenregister dan het modelreglement toelaat. De korpsen gaven veelal aan dat zij dit voor de uitvoering van hun werkzaamheden noodzakelijk achten.
7. logging database
Logging van de database bleek bij een enkel korps volledig te worden uitgevoerd. De meeste korpsen voerden aan dat de mogelijkheid daartoe niet wordt gebruikt omdat de performance van de systemen daardoor te zeer nadelig wordt beïnvloed.
8. verstrekkingen
Onderzocht is of de opname van informatie uit gespreksverslagen in andere CIE-registers tijdig had plaatsgevonden. Dat was steeds het geval. Wat betreft de vastgelegde verstrekkingen aan andere korpsen of aan tactische rechteerteams rezen geen vragen over de geoorloofdheid daarvan.
9. samenhang van inhoudelijke en technische/organisatorische aspecten
De hiervoor genoemde onderwerpen hebben afzonderlijk invloed op een goede en integere informatiehuishouding van de CIE. Tekortkomingen daarin kunnen grote gevolgen hebben voor de opsporing en vervolging enerzijds en het privacybelang van de geregistreerde anderzijds. Dat geldt temeer waar meerdere tekortkomingen zijn geconstateerd, aangezien deze elkaar versterken. Een samenloop van tekortkomingen heeft het CBP in het onderzoek meerdere malen geconstateerd. Essentieel is dan ook dat de informatiehuishouding zo wordt ingericht dat de risico's voor met name de betrouwbaarheid en integriteit van de informatie en de veiligheid van personen zo veel mogelijk worden beperkt.

I. Inleiding

Het College bescherming persoonsgegevens (CBP) is in de tweede helft van 2003 gestart met onderzoeken naar de bijzondere politieregisters van een achttal Criminele Inlichtingen Eenheden (CIE) bij de regionale politiekorpsen. Deze onderzoeken zijn tevoren schriftelijk aangekondigd aan alle korpsen via de portefeuillehouder privacy van de Raad van Hoofdd commissarissen. Het CBP heeft de selectie van de onderzochte korpsen gemaakt op basis van landelijke spreiding en diversiteit in korpsgrootte.

De onderzoeken hadden betrekking op het informantenregister, het register zware criminaliteit en het voorlopig register. Gelet op de gevoeligheid van de in deze registers verwerkte persoonsgegevens en de afscherming daarvan voor anderen, onder wie niet alleen geregistreerden, maar ook de rechter, is extern toezicht van groot belang. Aangezien naast politie en openbaar ministerie slechts het CBP als toezichthouder de mogelijkheid heeft van de inhoud van de CIE-registers kennis te nemen, ziet het CBP in deze positie een bijzondere verplichting om met name ook toe te zien op de inhoud van de bijzondere politieregisters.

De politieregisters bij de voorgangers van de CIE'en, de Criminele Inlichtingen Diensten, zijn onderwerp geweest van uitvoerige parlementaire discussie, die heeft geleid tot de Wet bijzondere politieregisters die in de Wet politieregisters (Wpolr) is geïncorporeerd. Deze Wet bijzondere politieregisters beoogt een zorgvuldige en rechtmatige verwerking van persoonsgegevens door de CIE te bevorderen. In dit kader is ook de Circulaire toezicht op beheer bijzondere politieregisters tot stand gekomen. Op grond van deze circulaire heeft inmiddels een zelfevaluatie met review plaatsgevonden. Deze richtte zich hoofdzakelijk op de organisatie van het beheer. In het kader van de review werd geen kennis genomen van de inhoud van de registers. Het CBP heeft van de uitkomsten van de zelfevaluatie met review betreffende de afzonderlijke korpsen geen kennis genomen, wel van de algemene slotevaluatie van 2 april 2003 die op alle onderzochte CIE'en betrekking had.

Het CBP heeft slechts een beperkte toets uitgevoerd. Het onderzoek naar de inhoud van de registers had het karakter van een steekproef. De onderzoekers van het CBP hebben gedurende een dag een bezoek ter plaatse gebracht aan de betreffende CIE. Vanwege deze beperking betrof het aantal onderzochte gespreksverslagen en mutaties een gering aantal. Daarnaast zijn technische en organisatorische aspecten van de CIE onderzocht. Deze geven belangrijke aanvullende informatie op het beeld van de gegevensverwerkingen door de CIE'en en worden dan ook in samenhang met die bevindingen besproken.

Het onderzoek en de beoordeling van de uitkomsten daarvan hebben zich hoofdzakelijk gericht op de volgende onderwerpen:

1. de opnamecriteria;
2. de juistheid en volledigheid van geregistreerde gegevens;
3. de vastlegging van gegevens uit het informantenregister in het voorlopig register respectievelijk het register zware criminaliteit;
4. de geoorloofdheid van geconstateerde verstrekkingen uit het register zware criminaliteit en het voorlopig register;
5. de maximale bewaartermijnen voor het register zware criminaliteit en het voorlopig register.

Tevens heeft de beoordeling zich gericht op de technische en organisatorische voorzieningen die in dit verband zijn genomen en ten slotte van mogelijk opvallende aspecten als het in de verwerkingen gebezigde taalgebruik.

Het CBP heeft van het onderzoek ter plaatse verslag opgemaakt. Na afloop van alle onderzoeken zijn de voorlopige beoordelingen per korps opgesteld en voorgelegd aan de desbetreffende korpsbeheerders. De reacties van de korpsbeheerders zijn verwerkt in de definitieve beoordelingen. Op basis van alle acht beoordelingen zijn deze algemene bevindingen opgesteld, die aan de verantwoordelijke ministers, van Binnenlandse Zaken en Koninkrijksrelaties en van Justitie, worden aangeboden. Hierna worden de algemene bevindingen openbaar gemaakt. In de wijze van publicatie verdisconteert het CBP de gevoeligheid van de onderzochte registers.

II. Bevindingen naar aanleiding van de onderzoeken

De belangrijkste algemene bevindingen zal het CBP bespreken op basis van de volgende indeling. De aspecten die naar het oordeel van het CBP deel uitmaken van de kern van de verwerkingen van gevoelige informatie door de CIE zijn onder A geplaatst. De onder B genoemde aspecten vormen waarborgen ter bevordering van de integriteit van de verslaglegging en ter afscherming en controle van de informatie. Onder C worden de interne verstrekkingen van het bruto-gespreksverslag met de informant naar het nettoverslag in het register zware criminaliteit en het voorlopig register alsmede verstrekkingen buiten de onderzochte CIE besproken. Ten slotte wordt onder D de samenhang tussen de inhoudelijke en de technische en organisatorische aspecten belicht.

- A
 - 1. inhoud van de gegevens (juistheid en volledigheid, overeenstemming bruto-netto, taalgebruik)
 - 2. codering (juistheid en volledigheid codering, doorvoeren nieuwe codering)
 - 3. bewaartermijnen (naleving maximale termijn)
 - 4. onderscheid in categorieën geregistreerden (verdachte, betrokkene, contacten)
- B
 - 5. definitieve vaststelling gespreksverslagen
 - 6. toegang (autorisaties)
 - 7. logging database
- C
 - 8. verstrekkingen (intern en extern)
- D
 - 9. samenhang van inhoudelijke en technische/organisatorische aspecten

A. 1. Inhoud gegevens

In het belang van een goede en effectieve opsporing en vervolging van strafbare feiten enerzijds en in het belang van de geregistreerden anderzijds, dienen de in de onderzochte registers verwerkte gegevens zo juist en volledig mogelijk te zijn. Het CBP heeft marginaal beoordeeld of de gespreksverslagen in het informantenregister voor het doel van het register, in het bijzonder het afleggen van verantwoording over het gebruik van de vastgelegde gegevens, voldoende gegevens bevatten. Hiervoor is de betrouwbaarheid van de gegevens van groot belang. Voor het vormen van een oordeel omtrent de betrouwbaarheid van criminele inlichtingen zijn de redenen van wetenschap en de juistheid van toetsbare informatie leidend.

Bij de toetsing van de juistheid en volledigheid van de in het register zware criminaliteit en het voorlopig register opgenomen gegevens heeft het onderzoek zich toegespitst op vergelijking van de mutaties met gegevens die van informanten werden verkregen met de desbetreffende gespreksverslagen in het informantenregister, de vergelijking van de zogenaamde netto- en brutoverslagen. Het CBP heeft er daarnaast op gelet of geen andere informatie werd aangetroffen dan de informatie die de CIE gerechtigd is te verwerken. Ook heeft het CBP gelet op het in de verslagen gebezigde taalgebruik, met name of dit voldoende duidelijk en zakelijk is en geen suggestieve of bijvoorbeeld denigrerende bewoordingen bevat.

Bij geen van de onderzochte korpsen werd in de registers informatie aangetroffen die niet door de CIE behoort te worden verwerkt. Over het geheel van de onderzochte gespreksverslagen en mutaties bezien kan geconcludeerd worden dat de inhoud in het overgrote deel van de gevallen consistent en voldoende duidelijk was. In enkele gevallen bleek aanvullende informatie nodig omdat de tekst van het gespreksverslag of de mutatie niet voldoende duidelijk was en op onderdelen vragen opriep, die pas na nadere toelichting konden worden opgehelderd. In andere gevallen bleek een conclusie niet overeen te stemmen met de daaraan voorafgaande opgenomen informatie of bevatte de mutatie in het register zware criminaliteit of het voorlopig register onvoldoende informatie om hieruit te kunnen afleiden of werd voldaan aan de opnamecriteria voor dat register.

Bij vergelijking van de bruto- en nettoverslagen stemde de inhoud daarvan in de meeste gevallen overeen. Bij sommige korpsen werd al in het informantenregister op overzichtelijke wijze het gespreksverslag ingedeeld in kant en klaar over te nemen passages ten behoeve van de opname in andere registers. In een enkel geval diende de tekst van de mutatie handmatig te worden vergeleken om te kunnen beoordelen uit welke combinatie van gespreksverslagen de informatie afkomstig was, waarbij ook enkele onjuistheden werden aangetroffen.

De vermelding van de redenen van wetenschap was bij de meeste korpsen voldoende duidelijk aangegeven. Bij enkele korpsen kwam uit de bevindingen naar voren dat meer aandacht aan de vermelding van de redenen van wetenschap kan worden besteed.

Het gebezigde taalgebruik werd in het algemeen zakelijk en adequaat geacht. In een enkel geval werd in gespreksverslagen jargon gebruikt. Aan het gebruik van jargon zijn risico's verbonden met name bij opname van de informatie in andere registers. Dit kan tot gevolg hebben dat de formulering een ongewenste betekenis in een andere context krijgt. Het CBP heeft in het onderzoek ook daadwerkelijk een geval aangetroffen waarin een algemeen gebruikte term door opname in het register zware criminaliteit in de context van geheel andere strafbare feiten kwam te staan en daarmee een andere betekenis kreeg dan deze term in het oorspronkelijke gespreksverslag had.

2. Codering

Het CBP heeft ook de codering van de informatie in het onderzoek betrokken. Daarbij valt onderscheid te maken tussen de verplicht voorgeschreven evaluatie- en afhandelingscodes die voor de uitwisseling tussen de CIE'en onderling gebruikt worden en bijvoorbeeld de in het informatiesysteem gebruikte mutatiecodes, aan de hand waarvan het mogelijk is vanuit het informantenregister zicht te houden op de gegevens die ook in een ander register zijn opgenomen. Voor zover het gebruikte systeem hiervoor een voorziening had werd van de laatstgenoemde vorm door de korpsen gebruik gemaakt.

Codering van criminele inlichtingen volgens de landelijk vastgestelde tabel is van groot belang, aangezien hierdoor inzicht wordt gegeven in de herkomst en wijze van verkrijging van de informatie. Deze codering vindt plaats volgens een tabel overeenkomstig bijlage I bij de CIE-regeling. Daarmee wordt ten eerste door middel van de evaluatiecode van de bron (informant) de betrouwbaarheid van de informant aangegeven volgens bepaalde categorieën (in letters). Die varieert van A - betrouwbaar, tot X – niet te beoordelen. Voorts wordt met behulp van een evaluatiecode van de informatie (in cijfers) aangegeven hoe de informatie moet worden beoordeeld. Volgens de oude coderingstabel (zie toelichting hierna) wordt aangegeven of de informatie bijvoorbeeld betrouwbaar wordt geacht of van horen zeggen is en vervolgens is bevestigd. Volgens de nieuwe tabel wordt daarmee aangegeven of de informatie door de informant zelf is waargenomen of bijvoorbeeld is gehoord van iemand die er zelf bij is geweest. Dit zegt iets over de “hardheid” van de informatie. Ten slotte wordt door middel van een afhandelingscode (in cijfers) aangegeven op welke wijze de informatie mag worden gebruikt, bijvoorbeeld ‘operationeel te gebruiken’ of ‘alleen te gebruiken in overleg met de afzender’.

Uit het onderzoek bleek dat de codering door alle korpsen consequent wordt vermeld. In veel gevallen wordt al in een zo vroeg mogelijk stadium gecodeerd, niet alleen in het register zware criminaliteit en het voorlopig register, vanuit welke registers verstrekking plaatsvindt, maar ook voor zover mogelijk in het informantenregister. Doorgaans kwamen de gehanteerde codes het CBP op grond van de informatie niet onaannemelijk voor. In een enkel geval bleek de codering onjuist.

De -verplicht voorgeschreven- coderingstabel is gewijzigd met ingang van 4 juli 2003. Bij vrijwel alle onderzochte korpsen bleken na 4 juli 2003 nog de oude codes te worden gebruikt. De korpsen gaven in de meeste gevallen aan dat het gebruikte informatiesysteem technisch niet de mogelijkheid tot aanpassing aan de nieuwe coderingstabel bood, dan wel dat aanpassing zeer kostbaar zou zijn. In afwachting van het nieuwe, landelijk in te voeren systeem Politie Suite Opsporing (PSO) geven deze korpsen aan het gebruikte systeem niet meer aanpassen aan de huidige regelgeving. Het CBP acht dit zorgelijk nu voor uitwisseling met andere CIE'en van belang is dat iedere CIE dezelfde coderingssystematiek hanteert. Bovendien dienen deze bijzondere registers een actueel en juist beeld te geven van de daarin opgenomen informatie.

Eén korps (gebruikmakend van het systeem RBS) bleek wel de nieuwe coderingswijze te hebben doorgevoerd. Twee andere korpsen (gebruikmakend van respectievelijk de systemen RBS en Octopus) hebben in hun reacties aangegeven het systeem in dit opzicht te zullen aanpassen. Gelet op deze bevindingen plaatst het CBP vraagtekens bij de houdbaarheid van de door andere korpsen aangevoerde argumentatie waarom aanpassing van de coderingstabellen niet mogelijk zou zijn.

3. Bewaartermijnen

Een effectieve opsporing is ermee gediend als de in het register opgenomen gegevens actueel zijn. In het belang van de geregistreerde dienen zijn gegevens niet nodeloos en eindeloos geregistreerd te blijven. Het CBP heeft zich in het onderzoek beperkt tot het toetsen van de maximale bewaartermijn die geldt voor het register zware criminaliteit (5 jaar) en voor het voorlopig register (6 maanden). De noodzaak tot registratie van de betrokkene binnen die termijn is slechts marginaal bezien.

Uit het onderzoek kwam in het geheel genomen, behoudens een afwijking in een enkel geval, geen overschrijding van de bewaartermijn in het register zware criminaliteit naar voren.

Bij de onderzochte mutaties in het voorlopig register daarentegen bleek meerdere malen sprake van enige overschrijding van de bewaartermijn. De overschrijding bedroeg echter niet meer dan enkele weken.

4. Onderscheid categorieën geregistreerden

De Wpolr bepaalt limitatief met betrekking tot welke categorieën van personen in het register zware criminaliteit persoonsgegevens mogen worden vastgelegd. Naast de opsporingsambtenaren, die in dit verband buiten beschouwing blijven, zijn dit de volgende personen:

1) verdachten (als bedoeld in artikel 27 Wetboek van Strafvordering) van misdrijven waarvoor het register is aangelegd;

2) betrokkenen, dat wil zeggen personen ten aanzien van wie een redelijk vermoeden bestaat dat zij betrokken zijn bij het beramen of plegen van misdrijven waarvoor het register is aangelegd;

3) contacten, te weten personen die in een bepaalde relatie staan tot verdachten of betrokkenen, in die zin dat zij andere dan toevallige contacten met deze personen hebben.

Onder deze laatste categorie kunnen tal van argeloze of minder argeloze personen vallen, zoals een criminele kompaan, maar ook de vader, de buurman of de zakenpartner van de geregistreerde verdachte of betrokkene. Contacten worden begrepen onder het begrip 'onverdachte personen'. Voor gegevens over deze personen gelden, voor zover deze verwerkt worden in een ander dan een bijzonder politieregister met als doel strafrechtelijke handhaving van de rechtsorde, een verkorte bewaartermijn van vier maanden.

In een voorlopig register worden gegevens opgenomen over personen over wie de beschikbare informatie nog niet voldoende is voor opnemings in het register zware criminaliteit, maar de verwachting bestaat dat zij uiteindelijk in samenhang met andere gegevens in het register zware criminaliteit kunnen worden opgenomen. Voor het voorlopig register geldt dezelfde indeling in categorieën personen, zij het dat het hierbij om 'aspirant'-verdachten, -betrokkenen en -contacten gaat.

Bovengenoemd onderscheid is met name van belang voor het verder gebruik in het strafrechtelijk circuit, nu ten aanzien van verdachten andere (dwang)middelen en rechten gelden dan voor betrokkenen. Ten aanzien van contacten geldt bovendien dat gegevens die op hen betrekking hebben maar beperkt mogen worden verstrekt. Het CBP is van oordeel dat een kwalificatie van een geregistreerde volgens het wettelijk kader uit het register, bijvoorbeeld de persoonskaart, dient te blijken om verschillende kwalificaties met betrekking tot dezelfde persoon te voorkomen.

Uit het onderzoek bleek dat bij geen enkel korps dit drieledig onderscheid wordt gemaakt. Bij de meeste korpsen wordt onderscheid gemaakt tussen twee categorieën geregistreerden: subjecten en contacten. Onder 'subject' wordt dan zowel de categorie verdachten als de categorie betrokkenen verstaan. Hiermee wordt weliswaar ten dele tegemoetgekomen aan het onderscheid dat tussen de verschillende wettelijke categorieën van geregistreerden dient te worden gemaakt, maar het CBP is van oordeel dat ook tussen betrokkenen en verdachten onderscheid dient te worden gemaakt. Immers, betrokkenen hebben te gelden als onverdachte personen, wat ten opzichte van verdachten de mogelijkheden beperkt de betreffende gegevens te verstrekken voor opname in een ander dan een bijzonder politieregister met als doel de strafrechtelijke handhaving van de rechtsorde.

Bij één van de korpsen werd zelfs op de persoonskaart van de geregistreerde in het geheel geen onderscheid tussen de categorieën gemaakt. Dit heeft tot gevolg dat alleen door kennis te

nemen van andere vastgelegde gegevens over een geregistreerde achterhaald kan worden of deze als verdachte, betrokkene danwel als contact is geregistreerd. Het spreekt voor zich dat dit eenvoudig tot misverstanden kan leiden of tot verschillende kwalificaties van dezelfde persoon ten aanzien van hetzelfde feit.

B 5. Definitieve vaststelling gespreksverslagen

Een aspect dat bijdraagt aan de integriteit van de verslaglegging is het voorzien in de mogelijkheid dat gespreksverslagen in het informantenregister na definitieve vaststelling daarvan in een later stadium niet meer kunnen worden gewijzigd. Het CBP acht dit een belangrijke waarborg tegen ongeautoriseerde wijziging van de informatie.

Uit het onderzoek kwam naar voren dat bij de meeste korpsen het gebruikte systeem latere wijziging niet uitsluit. Bij enkele korpsen is geconstateerd dat gespreksverslagen na vaststelling daarvan en fiattering door de leidinggevende, door middel van elektronische archivering definitief werden vastgelegd. In andere korpsen bestond deze mogelijkheid niet, maar waren interne procedures vastgesteld die bijdragen aan definitieve vaststelling van de verslaglegging, gebaseerd ofwel op interne discipline ofwel op een na verloop van enige tijd verhoogd autorisatieniveau, waardoor alleen de leidinggevende daarin wijziging kan aanbrengen. Inmiddels hebben enkele korpsen aangegeven dat een aanpassing in het systeem is ingevoerd waarmee gespreksverslagen definitief kunnen worden afgesloten. Het CBP acht het van belang dat voor deze functionaliteit meer aandacht wordt gevraagd.

6. Toegang

Op grond van het modelreglement informantenregister dienen er door de registerbeheerder voorzieningen van technische en organisatorische aard ter beveiliging van het register tegen verlies of aantasting van de gegevens en tegen onbevoegde kennisneming, wijziging of verstrekking daarvan te worden getroffen. In het modelreglement is vastgelegd dat slechts het hoofd van de CIE, zijn plaatsvervanger en de CIE-coördinatoren rechtstreeks toegang tot de informantenregisters mogen hebben.

Bij alle onderzochte CIE-en bleek dat naast de hiervoor genoemde functionarissen ook diverse andere medewerkers toegang hadden tot het informantenregister. Per korps bestonden hier aanzienlijke verschillen tussen, die ook samenhangen met de gekozen organisatie van de CIE binnen het korps. Deze ruime toegang is in strijd met het modelreglement. In alle gevallen hadden de runners toegang. Vaak ook waren administratief medewerkers of administratief gegevensbeheerders daartoe geautoriseerd.

Bij sommige korpsen waren tevens medewerkers van de infodesk, de RID of misdadaanalisten geautoriseerd tot het raadplegen van het register zware criminaliteit en het voorlopig register, zij het met een autorisatie van beperkt niveau, waardoor zij meestal niet tot niveau van embargo-informatie kunnen raadplegen. Hoewel voor deze ruime opvatting van autorisaties in de betreffende modelreglementen in samenhang met de CIE-regeling vooralsnog geen steun wordt gevonden, is het het CBP bekend dat hierover verschillende opvattingen bij de korpsen bestaan. Het CBP meent evenwel dat eenduidigheid op dit punt noodzakelijk is.

Algemeen geldt hier in ieder geval dat daar waar meer functionarissen geautoriseerd zijn tot een register, beheersrisico's voor de verwerkte informatie ontstaan.

7. Logging

De applicaties waarop de CIE-registers worden gevoerd verschillen in de mogelijkheden die zij bieden om uitgebreide logging van de database uit te voeren. Voor de afscherming van de informanten is het van belang zicht te houden op het gebruik van de gegevens in dit register.

Het geautomatiseerd bijhouden van de rechtstreekse toegang tot en het gebruik van de opgeslagen informatie is voorts van belang met het oog op de controle op de integriteit van het gegevensverkeer en zicht op een beheerste en juiste informatiehuishouding binnen de CIE.

Uit het onderzoek is gebleken dat veel van de onderzochte korpsen geen logging toepassen. Bij een groot deel van de korpsen voorziet de applicatie weliswaar in mogelijkheden tot logging, maar wordt daarvan geen gebruik gemaakt. De korpsen voeren daarvoor verschillende redenen aan. Veelal wordt erop gewezen dat het gebruik daarvan een nadelige invloed heeft op de performance van het systeem. In andere gevallen wordt er wel gelogd, maar is de weergave hiervan zo moeilijk leesbaar dat daarvan geen gebruik wordt gemaakt. In enkele gevallen wordt een beperkte logging uitgevoerd, waardoor bijvoorbeeld wordt bijgehouden wie wanneer op het netwerk inlogt. Het is dan achteraf niet mogelijk om te reconstrueren door wie welke gegevens uit het systeem zijn geraadpleegd of gewijzigd.

C 8. Verstrekkingen

Gelet op de gevoeligheid van de bij de CIE verwerkte informatie en de eisen die dat stelt aan het nauwgezet volgen van het geldende gesloten verstrekkingenregime, dient van alle verstrekkingen aantekening te worden gehouden. Het CBP heeft in het onderzoek de vastlegging van de verstrekkingen getoetst. De vastlegging van informatie uit het informantenregister in een ander politieregister binnen de CIE heeft het CBP hier gemakshalve als interne verstrekking aangeduid en de verstrekkingen buiten de CIE als externe verstrekking.

Wat betreft de interne verstrekkingen kunnen de in het informantenregister opgenomen inlichtingen, voor zover deze voldoen aan een doel van een ander politieregister, ook in dat andere politieregister worden vastgelegd. Deze opname in een ander politieregister dient plaats te vinden binnen vier maanden ingevolge de richtlijn van de procureurs-generaal van 8 januari 2002.

Uit het onderzoek volgde dat deze opname steeds binnen vier maanden is uitgevoerd en veelal zelfs binnen enkele dagen of hooguit binnen een maand.

Daarnaast bleek dat bij een aantal korpsen het vastleggen van verstrekkingen van de zogenaamde "bijvangst" gegevens, dat wil zeggen informatie uit gespreksverslagen in het informantenregister die vanwege hun inhoud niet in het register zware criminaliteit of het voorlopig register kunnen worden vastgelegd, een knelpunt te vormen. Een voorziening voor de registratie van dergelijke gegevens ontbreekt in de gebruikte systemen. Enkele korpsen hebben daartoe een aparte registratie aangelegd, maar het werd niet geheel duidelijk of deze registratie als onderdeel van een ander register of als een afzonderlijk register moest worden aangemerkt. In het laatste geval gelden wel de meldings- en reglementeringsverplichtingen van de Wpolr.

De toets die het CBP heeft aangelegd wat betreft de externe verstrekkingen is beperkt tot verstrekkingen die zijn vastgelegd en waarvan tijdens het onderzoek is gebleken. Het CBP heeft daarbij met name gelet op de vereiste codering en voorts op het beperkte verstrekkingenregime ten aanzien van contacten.

In het algemeen rezen geen vragen omtrent de geoorloofdheid van de vastgelegde verstrekkingen.

D **9. Samenhang van inhoudelijke en technische en organisatorische aspecten**

De hiervoor besproken onderwerpen hebben afzonderlijk invloed op een goede en integere informatiehuishouding van de CIE en vertegenwoordigen daarmee opsporings- en vervolgingsbelangen, maar ook het privacybelang van de geregistreerde. Tekortkomingen in een van deze aspecten kan aldus grote gevolgen hebben. Dit geldt temeer wanneer meerdere tekortkomingen worden geconstateerd, aangezien deze elkaar versterken.

Zo heeft het CBP onder meer een geval aangetroffen waarin inhoudelijke onjuistheden werden gesignaleerd in het gespreksverslag in het informantenregister, welke onjuistheid was overgenomen in de op basis daarvan opgemaakte mutatie in het voorlopig register; deze mutatie was bovendien langer dan de maximale termijn bewaard; voorts hadden meer medewerkers dan toegestaan toegang tot het informantenregister. In een ander geval bleek een mutatie ten onrechte opgenomen in het voorlopig register, terwijl de informatie ook inhoudelijk niet overeenstemde met het oorspronkelijke gespreksverslag; daarbij was de maximale bewaartermijn overschreden en had bovendien verstrekking van deze informatie plaatsgevonden aan een tactisch team.

Daar waar informatie niet adequaat wordt vastgelegd loopt de organisatie risico's die afbreuk doen aan met name de betrouwbaarheid en de integriteit van de informatie en de veiligheid van personen. Het is daarom van groot belang dat de informatiehuishouding zo is ingericht dat de kwaliteit en kwantiteit van de informatie, zoals de naleving van de bewaartermijnen en bijvoorbeeld de beperkte toegang tot de registers worden bewaakt. Essentieel hierbij is dat de bovengenoemde risico's zoveel mogelijk worden beperkt.

In het onderzoek is gebleken dat de technische en organisatorische aspecten in de praktijk niet altijd tegemoetkomen aan die risico's. Een ander voorbeeld hiervan vormt de bij alle korpsen aangetroffen praktijk dat het register zware criminaliteit en het voorlopig register geïntegreerd worden gevoerd in hetzelfde informatiesysteem. Het CBP heeft in beginsel geen bezwaar tegen het geïntegreerd voeren van beide registers, maar stelt daaraan de voorwaarden dat uit de registratie dient te blijken in welk register een geregistreerde is opgenomen en dat ook ten aanzien van alle geregistreerden de geldende regels nageleefd dienen te worden. Omdat bovengenoemd systeem bij het invoeren van gegevens niet direct dwingt voor één van beide registers te kiezen, maar de aanduiding van het toepasselijke register doorgaans eerst op de persoonskaart van de geregistreerde is opgenomen, blijft het risico aanwezig dat niet duidelijk is in welk register zich de informatie bevindt. In een enkel geval werd dan ook geconstateerd dat een aanduiding omtrent het register waarin de geregistreerde was opgenomen ontbrak.

Goede procedures en technische maatregelen kunnen de risico's van onjuiste informatie of ongeoorloofde toegang tot de informatie beperken en zo voldoende waarborgen bieden voor het op een zorgvuldige wijze verwerken van die gegevens.

III. De reacties van de korpsen

Aan de korpsbeheerders van de acht korpsen is bij toezending van de voorlopige beoordeling verzocht om een reactie, waarbij het CBP tevens verzocht aan te geven of, en zo ja welke maatregelen getroffen zullen worden ter herstel van de geconstateerde tekortkomingen. Uiteindelijk is van zeven korpsbeheerders een reactie ontvangen. Van één korps heeft de CIE-chef een reactie gestuurd, nadat een reactie door de korpsbeheerder was uitgebleven.

De meeste korpsen hebben gereageerd op de aandachtspunten die op de inhoud betrekking hebben in die zin, dat aangegeven wordt dat er aandacht aan zal worden besteed om het optreden van geconstateerde onvolkomenheden in het vervolg te voorkomen, bijvoorbeeld door het aanpassen van werkprocedures of door toezicht en controle door de CIE-leiding. Om in de toekomst overschrijding van de bewaartermijn te voorkomen heeft een aantal korpsen inmiddels maatregelen getroffen.

Wat betreft de aandachtspunten van meer technische en organisatorische aard heeft het CBP uiteenlopende reacties ontvangen. Ten aanzien van onder meer de aanpassing van de coderingstabel wordt in veel gevallen aangegeven dat in afwachting van de invoering van de landelijke applicatie geen aanpassingen meer in de systemen zullen worden uitgevoerd. Daartegenover staat dat enkele andere korpsen inmiddels de benodigde aanpassingen in het informatiesysteem hebben aangebracht. Een aantal korpsen heeft aangegeven het systeem aldus te hebben aangepast dat definitieve afsluiting van gespreksverslagen thans mogelijk is. Ten aanzien van de mogelijkheden van logging van de systemen wordt voornamelijk gewezen op de bezwaren en de technische onmogelijkheden die met het gebruikte systeem verband houden. Op het punt van de te ruime toegang tot het informantenregister is door enkele korpsen aangegeven dat men de huidige werkwijze noodzakelijk acht en derhalve niet aanpast. Andere korpsen hebben op dit punt in het geheel niet gereageerd. Ook met betrekking tot het vereiste onderscheid in wettelijke categorieën personen lopen de reacties uiteen van daar waar geen enkel onderscheid mogelijk blijft tot daar waar deze aanduiding aanvullend op het gedeeltelijke onderscheid dat reeds werd gemaakt zal worden opgenomen. Op lang niet alle onderdelen van de aandachtspunten is gereageerd. Een enkel korps heeft slechts een algemeen geformuleerde reactie gegeven. In de meeste gevallen is echter een gedetailleerde reactie op onderdelen gegeven.

IV. Conclusie

Het algemene beeld dat uit het onderzoek naar voren kwam is als overwegend positief aan te duiden. De onderzochte inhoudelijke aspecten bleken over het algemeen in orde. Wat betreft de onderzochte technische en organisatorische aspecten viel op dat op een aantal punten niet wordt voldaan aan de voorschriften die door de wet- en regelgeving worden gesteld. Veel van de korpsen geven aan dat zij, in afwachting van een landelijk in te voeren informatiesysteem, op die punten geen aanpassingen uitvoeren ten aanzien van de huidige systemen en gehanteerde werkwijzen.

De algemene bevindingen op de belangrijkste onderdelen kunnen als volgt worden omschreven.

1. inhoud van de gegevens

Het CBP heeft met name de juistheid en volledigheid van de informatie onderzocht en vergeleken of de in het register zware criminaliteit en het voorlopig register opgenomen mutaties (nettoverslagen) overeenkwamen met de gespreksverslagen in het informantenregister (brutoverslagen) waaruit zij afkomstig waren. Over het geheel genomen was de verslaglegging consistent en voldoende duidelijk en stemden de vergelijking van netto- en brutoverslagen overeen. Ook heeft het CBP geen informatie in de registers aangetroffen die niet door de CIE behoort te worden verwerkt.

2. codering

Het gebruik van de verplicht voorgeschreven evaluatie- en afhandelingscodes waarmee de CIE-informatie wordt gecodeerd is getoetst. Codering bleek door alle onderzochte korpsen consequent te worden vermeld en kwam het CBP doorgaans niet onaannemelijk voor. De sedert 4 juli 2003 gewijzigde coderingstabel bleek echter slechts bij één korps te zijn ingevoerd. Twee andere korpsen gaven aan deze tabel alsnog te zullen hanteren.

3. bewaartermijnen

Het CBP heeft hier de maximale bewaartermijn (marginaal) getoetst die geldt voor het register zware criminaliteit (5 jaar) en voor het voorlopig register (6 maanden). In het register zware criminaliteit is vrijwel geen overschrijding aangetroffen. Bij het voorlopig register werd meerdere malen een betrekkelijk geringe overschrijding geconstateerd.

4. onderscheid in categorieën geregistreerden

De Wpolr schrijft voor dat wat betreft in het register zware criminaliteit en voorlopig register geregistreerde personen onderscheid moet worden gemaakt tussen verdachten, betrokkenen en contacten. Geen van de onderzochte korpsen maakte dit driedig onderscheid. De meeste korpsen maken slechts onderscheid tussen subjecten (waaronder verdachten en betrokkenen begrepen worden) en contacten.

5. definitieve vaststelling gespreksverslagen

Bij de meeste korpsen bleek dat wijziging van gespreksverslagen na vaststelling daarvan niet door het systeem wordt uitgesloten. Door enkele korpsen is dit na het onderzoek alsnog aangepast.

6. toegang

Bij alle onderzochte korpsen bleek dat (veel) meer functionarissen rechtstreeks toegang hadden tot het informantenregister dan het modelreglement toelaat. De korpsen gaven veelal aan dat zij dit voor de uitvoering van hun werkzaamheden noodzakelijk achten.

7. logging database

Logging van de database bleek bij een enkel korps volledig te worden uitgevoerd. De meeste korpsen voerden aan dat de mogelijkheid daartoe niet wordt gebruikt omdat de performance van de systemen daardoor te zeer nadelig wordt beïnvloed.

8. verstrekkingen

Onderzocht is of de opname van informatie uit gespreksverslagen in andere CIE-registers tijdig had plaatsgevonden. Dat was steeds het geval. Wat betreft de vastgelegde verstrekkingen aan andere korpsen of aan tactische recheteteams rezen geen vragen over de geoorloofdheid daarvan.

9. samenhang van inhoudelijke en technische/organisatorische aspecten

De hiervoor genoemde onderwerpen hebben afzonderlijk invloed op een goede en integere informatiehuishouding van de CIE. Tekortkomingen daarin kunnen grote gevolgen hebben voor de opsporing en vervolging enerzijds en het privacybelang van de geregistreerde anderzijds. Dat geldt temeer waar meerdere tekortkomingen zijn geconstateerd, aangezien deze elkaar versterken. Een samenloop van tekortkomingen heeft het CBP in het onderzoek meerdere malen geconstateerd. Essentieel is dan ook dat de informatiehuishouding zo wordt ingericht dat de risico's voor met name de betrouwbaarheid en integriteit van de informatie en de veiligheid van personen zo veel mogelijk worden beperkt.